International Journal of Research in Advent Technology, Vol.4, No.1, January 2016
E-ISSN: 2321-9637
Available online at www.ijrat.org

Virtual Machine Introspection under DoS/DDoS Attack

Neha Sharma,RahulHada
Departmentof Computer Engineering, Poornima University, Jaipur, Rajasthan
Email: neha.sharma28530@gmail.com, rahulhada@poornima.edu.in

Abstract-Today, world is moving from conventional technology to virtualization techniques. This new technology allows several virtual machines reside on a single host machine. The main advantage of this is maximum resource utilization. But every new technology have some pros and cons. Network attacks such as Denial of service(DoS) and Distributed Denial of service(DDoS) exhaust resources of host machine as well as virtual machine. Some of these resources are bandwidth, memory, computing power etc. In this paper, mitigation of DoS and DDoS is implemented using Iptables. Iptable security increases network load on machine so, network performance has been tuned with the help of window scaling.Experimental work included implementation of iptable connection limits for mitigating DoS and DDoS attack and analysis of bandwidth using window scaling option. Appropriate window size was chosen for maximum bandwidth utilization. Results provide security from DoS and DDoS as well as better network performance tuning.

Index Terms-Virtual Machine; Xen; DoS; DDoS; iptable connection limit; RWIN;

1. INTRODUCTION

Several new technologies are emerging day by day.Virtual machines (VMs) provides services and computational infrastructure to organizations is increasingly prevalent in the modern it industry. The main idea behind virtualization is maximum and optimum utilization of resources of servers. Virtualization has also made the dream of such utility computing platforms as cloud computing a reality but still security is a prominent issue for every organization. Major security headaches are attackers, virus, and worms etc. Today, virtual machine is found in almost everywhere, so they are more likely to get affected by attacks such as DoS and DDoS. Virtual infrastructure components are at risk of dos for two primary reasons: (1) resources such as bandwidth, processing power, and storage capacities are not unlimited and so dos attacks target these resources in order to disrupt systems and networks. (2) Internet security is highly interdependent and the weakest link in the chain may be controlled by someone else thus taking away the ability to be self-reliant as consequences of these attacks their performance degrade [1]. These attacks are very severe for host as well as virtual machines. So, their mitigation is very necessary so that machine can perform in a right way. Several useful mitigation techniques are there to reduce and prevent network attacks. Some of them are firewall, IP trackback, network ingress filtering, intrusion detection system etc.

In this paper host machine and virtual machine installed on Xen hypervisor is used as victim virtual machine. DoS and DDoS attacks scenario is created with another attacker machine. Iptable connection limit is used as preventive measure for these attacks.

A. Virtualization

Virtualization is a broad concept that refers to the creation of a virtual version of something, whether hardware, a software environment, storage, or a network. In a virtualized environment there are three major components: guest, host, and virtualization layer. There are three major type of virtualization: Para virtualization, full virtualization and hardware virtualization [8].

B. Xen

Xen is an open source initiative implementing a virtualization platform based on Para virtualization.. Para virtualization requires no special hardware to realize virtualization, instead relying on special kernels and drivers. There is an initial domain, called Domain0 (Host Machine) and other one is called Domain U (Virtual Machine) [8].

C. DoS/DDoS Attack

Gligor et al. [1] defined DoS as: “a group of otherwise authorized users of a specific service is said to deny service to another group of authorized users if the former group makes the specified service unavailable to the latter group for a period of time which exceeds the intended (and advertised) waiting time.”

In Distributed Denial of Service (DDoS) attacks, attackers do not use a single host for their attacks but a cluster of several dozens or even hundreds of computers to do a coordinated strike [1].

D. Iptables

Iptables is a rule based utility that uses policy chains to allow or block network traffic. When a connection tries to establish itself on a system, iptables looks for a rule in its list to match to it. If doesn’t find one, it

resorts to default action. Iptables connection limit modules allow users to restrict the number of parallel TCP connection to a server per client ip address. This is useful to protect server against attacks [9].

E. Window Scaling

Window scaling identifies the maximum amount of data a sender can transmit without receiving a window update via a TCP acknowledgement. The maximum amount of data can be sent to receiver without getting acknowledgement back is depends on a factor called receiver window size. By setting appropriate receiving window size on receiving end, network performance can be maximized [10].

In this paper,Xen hypervisor is used as virtual machinemanager on which virtual machine installed.DoS and DDoS attacks scenario is created with another attacker machine. For mitigation of these attacks, Iptable connection limit was used as preventive measures. Also, Network performance is maximized by setting appropriate receiving window size on receiving end.

The Paper is organized in following way: section II literature survey in DoS attack Detection. Section III described experimental setup. Section IV & V deal with implementations and results respectively. Section VI presents conclusion of the work.

2. RELATED WORK

BahaaQasim et-al, proposed DoS/DDoS attack detection technique using iptable firewall. Denial of service and distributed denial of service attack was defended using iptable. Advantage of this approach was cost effectiveness but iptable rules detected false positive in some cases and generate alarm even when there is no attack. The future scope in the area could be operwrt for writing iptable rules that target on router to mitigate DoS and DDoS attack [1].

Chirag N. Modi et-al, proposed novel security framework H-NIDS to detect network attacks in cloud computing by monitoring traffic. In the proposed approach anomaly based and signature based detection approaches were used to detect internal as well as external attack in cloud environment. Author compared Bayesian classification, associative classification, decision tree classification in terms of precision values & accuracy. Higher detection rate, higher accuracy and low false positive rate showed efficiency of technique [2].

Ryan Shea et-al, proposed performance analysis of virtualization under TCP based DOS attack using benchmark tools on different hypervisor. Performance of CPU, network, memory, and filesystem was analyzed under normal and attack conditions. Xen, KVM, and OpenVZ were chosen to be evaluated. KVM was found better and faster in DDoS detection. Limitation of this approach was hypervisor based detection was more expensive than system based approaches [3].

Samad S. Kolahi et-al, proposed analysis of UDP DDOS flood attack and defense mechanism on virtual web server. Impact of UDP attack on TCP throughput, round trip time, CPU utilization for web server was analyzed with access control list (ACL). CPU usage was 24.9% during attack and after applying the prevention mechanism, CP usage was reduced. Threshold limit reduced CPU up to 3%. IP and ACLs reduced the CPU usage up to 15%, while network load balancing decreased the CPU usage to 18%. [4].

XieChuiyia et-al, distributed intrusion detection system against flooding denial of services attacks. Data was gathered by all FIDS and analyzed by communicating each other. F-IDS were composed of traffic gathering module, traffic table, traffic matrix and communication module. Flooding attacks were detected by Traffic matrixes and local and global communications reduced the overhead of data exchanging [5].

Sara Mirzaie, et-al, proposed TCP SYN attack detection technique using iptable firewall. In proposed approach, attempts were made to limit the number of TCP connection request from any ip address. The rate of incoming SYN packets were limited. Specific number of SYN packet was sent within certain intervals and they were dropped if they exceeded the limit. Limitation of this approach was that drop rate of packet was quite high [6].

Zhuang Wei et-al, designed TCP DDOS attack detection architecture on the host in the KVM Virtual Machine Environment. This strategy detected attack of virtual machines in user mode indirectly by treating user mode as an independent virtual machine. After applying CUSUM algorithm, the fail rate and distorting rate was found almost zero [7].

Our proposed approach was better in a way because in spite of dropping network packet it limits network packets, we analyzed CPU usage and memory load during attack at host machine and analyzed window size for the network. To improve network bandwidth utilization receiving window scaling was scaled.

3. EXPERIMENTAL SETUP

DoS and DDoS attack was performed by attacker machine on victim machine

Table I Hardware Specifications

Processor	1.86GHz
Memory	4 GB

Virtualization	Hardware Assisted Virtualization Enabled

Table II Software Specifications

Attacker Machine OS	Backtrack5 r3
VMM	Xen 4.1
Host Operating System	Red Hat 6
Guest Operating System	Red Hat 6
Wireshark as packet capturing tool	-

4. IMPLEMENTATION

Implementation of experiment is divided into two parts as follows.

A. Attack Detection

From the attacker machine, UDP packets were flooded to launch DoS attack on victim virtual machine. During the DoS attack, system resources (CPU and Memory) of host machine are totally consumed in serving attacker's invalid. At the same time, legitimate requests will not be served as victim will be busy in serving attacker's invalid requests. CPU and Memory Load on DOM 0 wasanalyzed during attack.

DDoS attack has been done on virtual machine. There were four malicious attacker node are generated by attacker machine to flood TCP Packets. This made multiple connections at virtual machine on port 80.

To detect DOS and DDOS attacks, iptable rules were applied so that attack packets is can be detected and appropriate action is to be taken such as log attack packet and alert generation.If incoming packet match the rule criteria than log of these packet and alert is generated at the screen.

B. Network Performance Analysis under Attack

Firewalls, load balancers, IDS put some extra load on system resources and network performance, so by paying attention on TCP receiving window size, performance of low fat network can be tuned.

TCP receiving window size(RWIN) =BW X delay
In this experimental scenario, Network bandwidth was 100 mbps & Delay is 17ms. So,

RWIN= 100*10^6 *17*10^-3/8=212.5 KB

The product of bandwidth and delay shows the amount must be transmitted, to efficiently use the connection speed As, operating system has this default value is 65535 bytes (65 KB), the connection is not fully utilized. So, if we calculate 212.5-65=147.5 KB was left unused. To solve this problem, there is need of use higher window size. For this, TCP window scaling option was enabled by doing changes in system files.

5. RESULTS AND DISCUSSION

The experiment results were interpreted in the form of statistical graphs and the results were analyzed with various statistical comparisons in accordance to a few of our intriguing cases.

Table IIICPU Load on DOM0 under DoS attack

Time (min)	Read Cycle (sec/s)
1	65
2	450
3	928
4	1264
5	2650
6	3509
7	3717
8	3900
9	4483
10	4804

All our interpreted results were presented as an average value of the obtained data after repeating the experiment for a significant number of values.

Table IV Memory Load on DOM 0 under DoS

Time (min)	Memory Load(KB)
1	25
2	198
3	314
4	488
5	609
6	839
7	925
8	1194
9	1272
10	1408

Table III& IV shows CPU Load and Memory Load under the DoS attack respectively. Duration of attack was around 10 minutes.

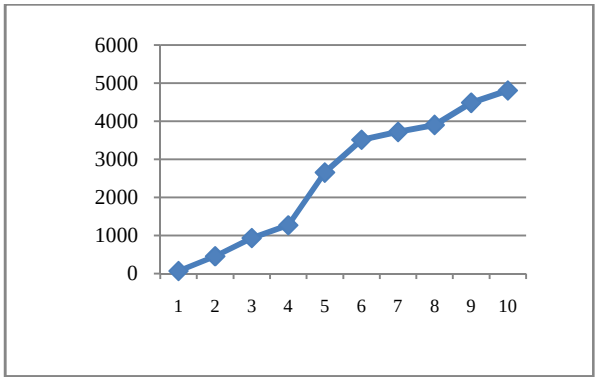

Fig 1: CPU Load on DOM0 during DOS Attack

Fig 1 shows graph between time and CPU read cycle. Initially, system was in idle state, there was no load on CPU but as the number of packets increases, Load on CPU increases. Read cycle reach up to 4804 sec/s during attack.

Fig 2 shows graph between time and Memory Load. Initially, system is in idle state, there was no load on memory but as the number of packets increases, Memory load increased and reach up to 1408 KB.

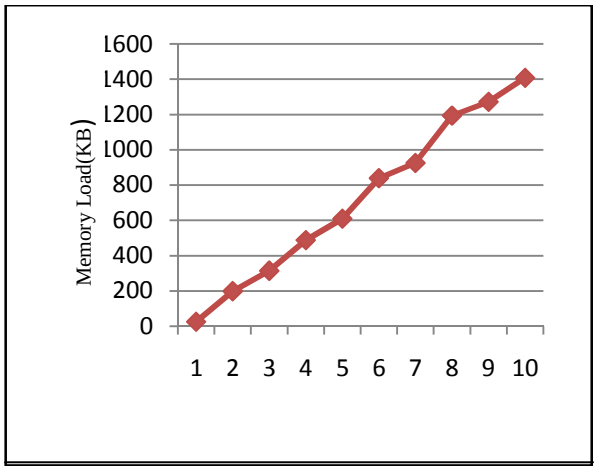

Fig 2: Memory Load on DOM0 during DOS Attack

Table V & VI shows CPU Load and Memory Load under the DDoS attack respectively.

Table VCPU Load on DOM0under DDoS

Time (min)	Read Cycle (sec/s)
1	53
2	120
3	500
4	1265
5	1596
6	2109
7	2400
8	3566
9	4566
10	7046

Table VI Memory Load on DOM 0 under DDoS

Time (min)	Memory Load(KB)
1	52
2	210
3	405
4	499
5	615
6	932
7	1266
8	1403
9	1605
10	1965

Fig 3 shows graph between time and CPU read cycle. Initially, system is in idle state, there is no load on CPU but as number of SYN request come again and again, CPU become busy in serving false requests and read cycle reach up to 7046 sec/s.

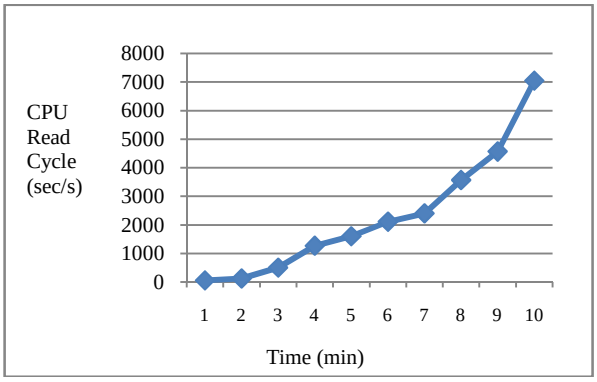

Fig 3: CPU Load on DOM0 during DOS Attack

DDoS attack put more load on memory rather than DoS. Fig 4 shows memory load per minute under the DDoS attack.

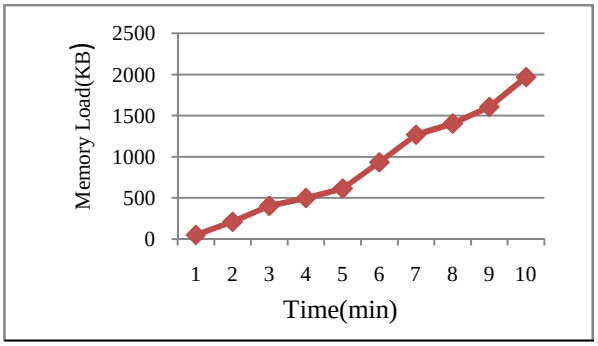

Fig 4: Memory Load on DOM0 during DDOS Attack

More packets put more load on memory and sometimes causes system or memory crash.

A. Calculation of Appropriate Window Size for Performance Tuning

The interval of scaling window size was calculated by the formula 2^s*65535, where s is called scale factor. By varying the value of s=1, 2,3,4,5 receiving window can be scaled as per need. Table VII shows relation between different window size and link utilization:

Table VII Scaling RWIN Window

Value of Scale factor	RWIN=2^s*65535	Difference between calculated RWIN and standard RWIN	Solution Feasibility
s=0	65KB	212.50-65=147KB	Not Feasible
s=1	131.07KB	212.50-131.50=81KB	Not Feasible
s=2	262.14KB	262.14-212.50=49 KB	Feasible
s=3	524.28KB	524.28-212.50=311.78 KB	Not Feasible
s=4	1048.56KB	1048.56-212.50=836.06 KB	Not Feasible

The value of calculated RWIN was greater or nearly equal to standard values. In table VII difference between calculated and standard window size is given. For s=2, this difference is minimum or we can say calculate RWIN(212.50KB) was nearly equal to Standard window size(262.50).So, putting s=2, gives feasible solution.

6. CONCLUSION

In this work, capability of iptables was explored to defend against the attacks. To determine whether the network traffic was legitimate or not, iptables relies on a set of rules, these rules tell whether to consider as legitimate and what to do with the network traffic coming from a certain source, going to a certain destination, or having a certain protocol type. Result showed effectiveness of iptables against these attack as well as network performance was also maintained with the help of window scaling. This work can be extended further by using advanced features of Iptables such as NAT, IP masquerading, packet redirect in future.

ACKNOWLEDGEMENT

I would like to express my deep gratitude and thanks to **Dr. Mahesh Bundele (Coordinator, Research), Poornima University** for giving me an opportunity to work under his guidance for review of research papers and his consistent motivation & direction in this regard. I would also express my sincere thanks to **Mr. Rahul Hada (Associate Professor, CE), Poornima University** for their guidance and support.

REFERENCES

[1] BahaaQasim; M. AL-Musawi (2012): Mitigating Dos/Ddos Attacks Using Iptables, International Journal of Engineering & Technology IJET-IJENS Vol: 12 No: 03,pp 101-111

[2] Chirag N. Modi; Prof Dhiren Pate l(2013), A Noval Hybrid Network Intrusion Detection System (H-IDS) in cloud computing, IEEE 2013, pp 23-31.

[3] Mirzaie, S.; Elyato, A.K.; Sarram, M.A(2010), Preventing of SYN Flood Attack with Iptables Firewall, Communication Software and Networks, 2010. ICCSN '10. Second International Conference on , vol., no., pp.532,535.

[4] Shea .R.; Jiang Chuan Liu (2012), Understanding the Impact of Denial of Service Attacks on Virtual Machines, Advance Computing Conference, 2012. IACC 2012. IEEE International, vol., no., pp.1170, 1172.

[5] Samad S. Kolahi, KiattikulTreseangrat (2015), Analysis of UDP DDoS Flood Cyber Attack and Defense Mechanisms on Web Server with Linux Ubuntu 13, IEEE 2015

[6] XieChuiyi; Zhang Yizhi; Bai Yuan; LuoShuoshan; Xu Qin, "A Distributed Intrusion Detection System against flooding Denial of Services attacks," Advanced Communication Technology (ICACT), 2011 13th International Conference on , vol., no., pp.878,881,Feb. 2011

[7] Zhuang Wei; GuiXiaolin; Huang Ru Wei; Yu Si (2012), TCP DDOS Attack Detection on the Host in the KVM Virtual Machine Environment, Computer and Information Science (ICIS), 2012 IEEE/ACIS 11th International Conference on , vol., no., pp.62,67.

[8] RajKumarBuyya, CristianVecchiola, S. ThamariaSelvi,"Mastering cloud computing, Fundamentals and Application Programming"

[9] http://stackoverflow.net/iptables

[10] http://github.com/window_scaling